UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/805,279	03/13/2001	Robert M. Barnhart	SAIC0039	1264

75131 7590 12/16/2009

KING & SPALDING LLP (SAIC CUSTOMER NUMBER)
ATTN: DAWN-MARIE BEY
1700 PENNSYLVANIA AVE, NW
SUITE 200
WASHINGTON, DC 20006

EXAMINER	
JARRETT, SCOTT L	

ART UNIT	PAPER NUMBER
3624	

MAIL DATE	DELIVERY MODE
12/16/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/805,279
Filing Date: March 13, 2001
Appellant(s): BARNHART, ROBERT M.

Mr. John Harrington Reg. No. 25,592

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed November 2, 2009 appealing from the Office action mailed June 4, 2009.

(1) Real Part in Interest

A statement identifying by name the real party of interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

20020077887 Shrader et al. 6-2002

Cranor et al., Design and Implementation of a Practical Security-Conscious Electronic Polling System, Proceedings of the Hawaii International Conference of System Sciences, 1997

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

The ground(s) for rejection are reproduced below from the Final Office Action, mailed June 3, 2008, and are provided here for the convenience of both the Appellant and the Board of Patent Appeals:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 29-30 and 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Shrader et al., U.S. Patent Publication No. 2002/0077887.

Regarding Claims 29 and 33 Shrader et al. teach a method and system for assisting a user in verifying a cast ballot recorded (saved, stored, executed, etc.) in a system (server) comprising (Abstract; Paragraphs 0050-0053; 0060-0063; Figures 4-8):

- forming (generating, creating, signing, encrypting, etc.) a digital signature of a cast ballot using the private key of a system (server; "The voting tabulator *signs, encrypts and sends the encrypted electronic ballot* to the voting mediator 72 in a message that is encrypted with the voting mediator's public key and signed with the *validator's private key*; Paragraph 0063; Figures 7-8, Element 72);

- associating (storing, linking, relating, etc.) the cast ballot, the voter's digital signature of the ballot with a ballot number (vote serial number, unique number/unique identifier, etc.; validating ballot request; Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71);

- forming a message (confirmation, string, receipt, acknowledgement, token, etc.) comprising a system's digital signature of the ballot and the ballot number (verification message(s) exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8);

- making the message available (verification message exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8);

- receiving the message (verification message(s) exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8, Elements 72-74);

- extracting (decrypting, stripping, de-signing, deciphering, etc.) the ballot number and the system's digital signature from the message (verification message(s) exchanged between tabulator to mediator; Paragraph 0063; Figures 7-8, Elements 73-75);

- for vote serial number comparing the system's digital signature of the ballot received to the system's digital signature of the ballot (Paragraphs 0061-0063; Figures 7-8); and

- *if* the comparison shows equivalency (match, consistency, equality, etc.) determining that cast ballot (message, token, etc.) is verified (valid, authentic, genuine, unaltered, secure, etc.; Paragraphs 0061, 0063; Figures 7-8).

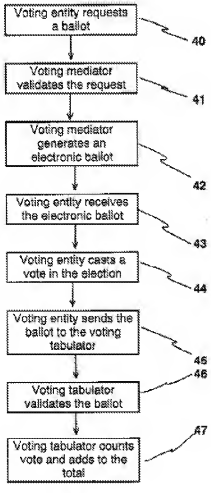
Voting entity requests a ballot
40
Voting mediator validates the request
41
Voting mediator generates an electronic ballot
42
Voting entity receives the electronic ballot
43
Voting entity casts a vote in the election
44
Voting entity sends the ballot to the voting tabulator
45
Voting tabulator validates the ballot
46
Voting tabulator counts vote and adds to the total
47

FIG. 4

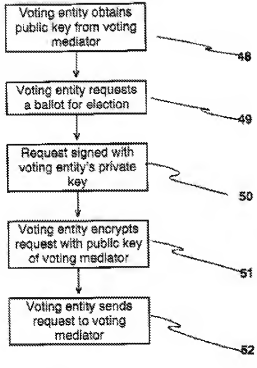
Voting entity obtains public key from voting mediator
48
Voting entity requests a ballot for election
49
Request signed with voting entity's private key
50
Voting entity encrypts request with public key of voting mediator
51
Voting entity sends request to voting mediator
52

FIG. 5

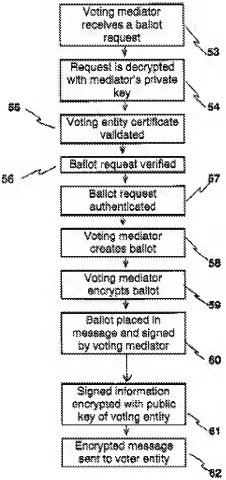
Voting mediator receives a ballot request
53
Request is decrypted with mediator's private key
54
55
Voting entity certificate validated
56
Ballot request verified
57
Ballot request authenticated
Voting mediator creates ballot
58
Voting mediator encrypts ballot
59
Ballot placed in message and signed by voting mediator
60
Signed information encrypted with public key of voting entity
61
Encrypted message sent to voter entity
62

FIG. 6

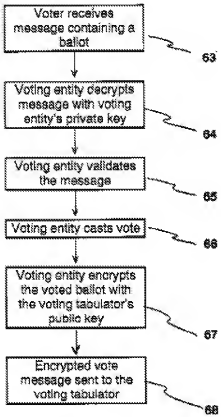
Voter receives message containing a ballot
63
Voting entity decrypts message with voting entity's private key
64
Voting entity validates the message
65
Voting entity casts vote
66
Voting entity encrypts the voted ballot with the voting tabulator's public key
67
Encrypted vote message sent to the voting tabulator
68

FIG. 7

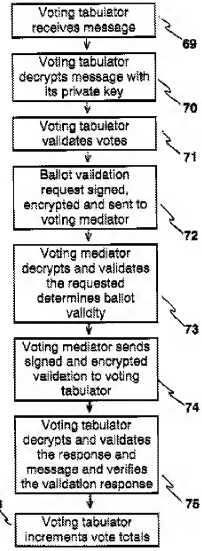

FIG. 8

Regarding Claim 30 Shrader et al. teach a method and system for assisting a user in verifying a ballot recorded in a system wherein the message (confirmation token, received token) further comprises the system's digital signature of the ballot and ballot number (aggregation; Paragraphs 0060-0062; Figure 2, Certificate No.); and wherein the method further comprises the steps of:

- extracting a digital signature of the ballot and ballot number (aggregation) from the message (received token; Paragraphs 0060, 0061, 0063; Figures 6-8); and

- the cast ballot is verified only upon the additional condition that the server's received digital signature of the aggregation is equivalent to the server's digital signature of the aggregation (Paragraphs 0061, 0063; Figures 6-8; Elements 67-75).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cranor et al., Design and Implementation of a Practical Security-Conscious Electronic Polling System (1996) in view of Shrader et al., U.S. Patent Publication No. 2002/0077887.

Regarding Claim 31 Cranor et al. teach a method and system for assisting a user in verifying (validating, authenticating, certifying, etc.) a cast ballot (vote) recorded (saved, stored, etc.) in a server (system) the method/system comprising (Abstract; Figures 1,3):

- receiving, in a system (server, computer, terminal, device, etc.), at least one set of a cast ballot and a voter's digital signature of the ballot (Paragraph 2, Page 5);

- forming (generating, creating, signing, encrypting, etc.) a digital signature of the ballot using the private key of a system (Paragraph 2, Page 5);

- associating (storing, linking, relating, etc.) the cast ballot, voter's digital signature of the ballot and the voter's identification number (Paragraphs 3-4, Page 7);

- forming a message (confirmation token, string, receipt, acknowledgement, etc.) comprising system's digital signature of the cast ballot, the voter's digital signature of the cast ballot, and the system's digital signature of the aggregation of the cast ballot, the voter's digital signature of the ballot and the system's digital signature of the ballot ("validator", "tallier", "validation certificate", "receipt"; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- making the message (token, string, etc.) available to a user (entity, voter, system, subsystem, third party, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- receiving the messages (confirmation, token, verification, acknowledgement, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- extracting (decrypting, stripping, etc.) *at least one of the following* from the message Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1):

  - voter's digital signature of the ballot; ***or***

  - system's digital signature of the ballot; ***or***

- system's digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation);

- for extracted ballot number and the corresponding ballot number comparing *at least one of the following* (Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1):

  - voter's digital signature of the ballot extracted from the message and voter's digital signature of the ballot; ***or***
  - system's digital signature of the ballot extracted from the message and system's digital signature of the ballot, ***or***
  - system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation) extracted from the message and system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation); and

- *if* the comparison shows equivalency (match, consistency, equality, etc.) determining that the cast ballot is verified (valid, authentic, genuine, unaltered, accepted, counted, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1).

Cranor et al. further teaches individual verifiability (Paragraphs 1-2, Page 12) as well as a unique vote/ballot identifier (receipt number/#; Figure 1, Pages 3-4; Page 8; db index, Paragraph 1, Page 11).

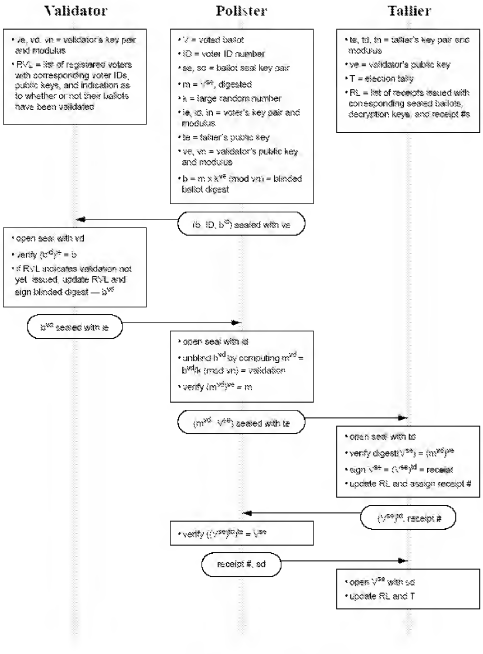

Figure 1: Blind Signature Protocol Overview

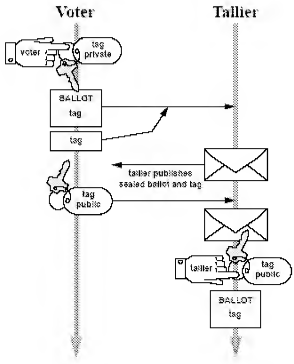

Figure 3: Phase 2 of the Two Agency Protocol

Cranor et al. teaches a system and method for voting securely over a network comprising *associating at least two unique identifiers with ballots cast by voters* wherein the unique identifiers (vote serial numbers) are generated and associated with the cast ballot only *after* the voters casts their ballot containing their choices (receipt number: Paragraphs 3-4, Page 8; Figure 1; index number for uniquely identifying, accessing and storing cast ballots in a database, Paragraph 4, Page 8)

Our tallier computes a 16-byte digest of *each encrypted ballot received* and uses it *to index the encrypted ballots and receipts*. A hash table could be added for greater efficiency in *looking up encrypted ballots*. This modification is probably necessary to accommodate large-scale elections. (emphasis added, Paragraph 4, Page 8)

While the use of unique identifiers for (paper and/or electronic) ballots is a common practice Cranor et al. does not expressly teach that the cast ballot contains a vote serial number as claimed.

Shrader et al. teach that ballots comprise a vote serial number (unique ballot ID, certificate no.) in an analogous art of secure electronic voting/balloting over a network for the purposes of ensuring voters only cast their ballot once (Paragraph 0061; Figures 2, 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71).

It would have been obvious to one skilled in the art at the time of the invention that the system and method for verifying a cast ballot recorded on a system (server) as taught by Cranor et al. would have benefited from including in the ballot a unique ballot identifier (vote serial number) in view of the teachings of Shrader et al.; the resultant system/method providing an additional mechanism for ensuring that valid voters only vote once (Shrader et al.: Paragraph 0063).

Regarding Claim 32 Cranor et al. teach a method and system for verifying a cast ballot recorded in a system further comprising if the comparison shows equivalence between the system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, extracted from the

message and system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot and the system's digital signature of the ballot (aggregation) determining that the message (token) has not been modified (altered, disturbed, edited, etc.) since its formation (Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8).

Cranor et al. does not expressly teach that ballots further comprise vote serial numbers as claimed.

Shrader et al. teach that ballots comprise a vote serial number (unique ballot ID) in an analogous art of secure electronic voting/balloting for the purposes of ensuring voters only cast their ballot once (Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71).

It would have been obvious to one skilled in the art at the time of the invention that the system and method for verifying a cast ballot recorded on a system (server) as taught by Cranor et al. would have benefited from including in the ballot a unique ballot identifier (vote serial number) in view of the teachings of Shrader et al.; the resultant system/method providing an additional mechanism for ensuring that valid voters only cast their ballot once (Shrader et al.: Paragraph 0063).

(10) Response to Argument

In Applicant's remarks filed January 13, 2009 Applicant's argues that:

- the examiner mischaracterizes the claim language specifically B_{cast} (Bullets 1-2, Page 5; Bullet 1, Page 12);

- that the prior art of record fails to teach or suggest each and every element of the claimed invention, specifically that Shrader et al. and/or Cranor et al. fail to teach or suggest:

- assisting a user in verifying a cast ballot stored in a server (Last Bullet, Page 9; Second to last Paragraph, Page 10);

- forming a digital signature of B_{cast} using a private key of the server (Last Bullet, Page 10);

- associating the B_{cast} and DS(B_{cast}, S) with a vote serial number (Bullet 1, Page 11);

- forming a confirmation token comprising DS(B_{cast}, S) and the vote serial number (Last Bullet, Page 12);

- making the confirmation token available to a user (Bullet 1, Page 10; Bullet 1, Page 13); and

- if the comparison shows equivalence (Claim 29, 31, 33) determining that B_{cast} is verified (Last Bullet, Page 13).

In response to Applicant's argument that the examiner mischaracterizes the claim language and further that the prior art of record fails to teach or suggest associating a vote serial number with B_{cast}, the examiner respectfully disagrees.

Nothing in the claimed method steps specifically recites when or how a vote serial number is generated or subsequently associated with a Ballot. Further nothing in the invention as claimed precludes the assignment of a vote serial number to a ballot before, during or after the ballot has been cast, delivered (e.g. sent to a voter/user) or otherwise acted upon. Further Applicant's own disclosure teaches that the vote serial number is just an incidental sequence number (Paragraph 0054).

Examiner has interpreted the claim to read that a Ballot has an vote serial number associated with it and it is that vote serial number, regardless of when or how it was associated with the Ballot, that is used in the subsequent method steps for forming/making and comparing the various tokens/keys.

Shrader et al. teach associating a Vote Serial Number to a cast Ballot (one that has been delivered to a user; vote serial number, unique number/unique identifier, etc.; validating ballot request; Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71).

Cranor et al. teach associating the cast ballot with a vote serial number (Paragraphs 3-7, Page 7; receipt number/#; Figure 1, Pages 3-4; Page 8; db index, Paragraph 1, Page 11).

In response to Applicant's argument that the prior art of record fails to teach or suggest assisting a user verify a ballot stored in a server the examiner respectfully disagrees. The recitation "assisting a user verify a ballot stored in a server" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Cranor et al. (individual verifiability; Paragraphs 1-2, Page 12).

In response to Applicant's argument that the prior art of record fails to teach or suggest forming a digital signature of B_{cast} using a private key of the server the examiner respectfully disagrees.

Shrader et al. ("The voting tabulator *signs, encrypts and sends the encrypted electronic ballot* to the voting mediator 72 in a message that is encrypted with the voting mediator's public key and signed with the *validator's private key*; Paragraph 0063; Figures 7-8, Element 72).

In response to Applicant's argument that the prior art of record fails to teach or suggest forming a confirmation token comprising DS(B_{cast}, S) and the vote serial number the examiner respectfully disagrees.

Shrader et al. (verification message(s) exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8).

Cranor et al. (Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1).

In response to Applicant's argument that the prior art of record fails to teach or suggest making the confirmation token available to a user the examiner respectfully disagrees.

Initially it is noted that the whether or not the confirmation token is made available to a user or not merely recites non-functional descriptive material wherein the method steps are performed in the same manner and result in the same result regardless of whether or not the confirmation token is made available to a user especially since the claims fail to state what, if anything, the user does or does not do upon the confirmation token being made available. Neither to the claims specifically recite what qualifies making the confirmation token available to a user (e..g. the token is in a human-readable format, posted on a web page, sent via an email, can be requested or viewed by the user, nearly anything within the computer systems of Shrader et al. and Cranor et al. qualify under the broad term of making available).

Shrader et al. (verification message exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8).

Cranor et al. (Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1).

In response to Applicant's argument that the prior art of record fails to teach or suggest that if the comparison shows equivalence determining that B_{cast} is verified the examiner respectfully disagrees.

Initially it is noted that the method steps comprises a conditional statement that which omits an essential step, i.e. what, if anything happens, if the comparison does not show equivalence wherein it is noted that the method step is not executed when the comparison is not equivalent.

Shrader et al. (Paragraphs 0061, 0063; Figures 7-8).

Cranor et al. (Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Scott L Jarrett/

Primary Examiner, Art Unit 3624

Conferees:

Vincent Millin/vm/

Appeals Conference Specialist

3600

/Bradley B Bayat/

Supervisory Patent Examiner, Art Unit 3624